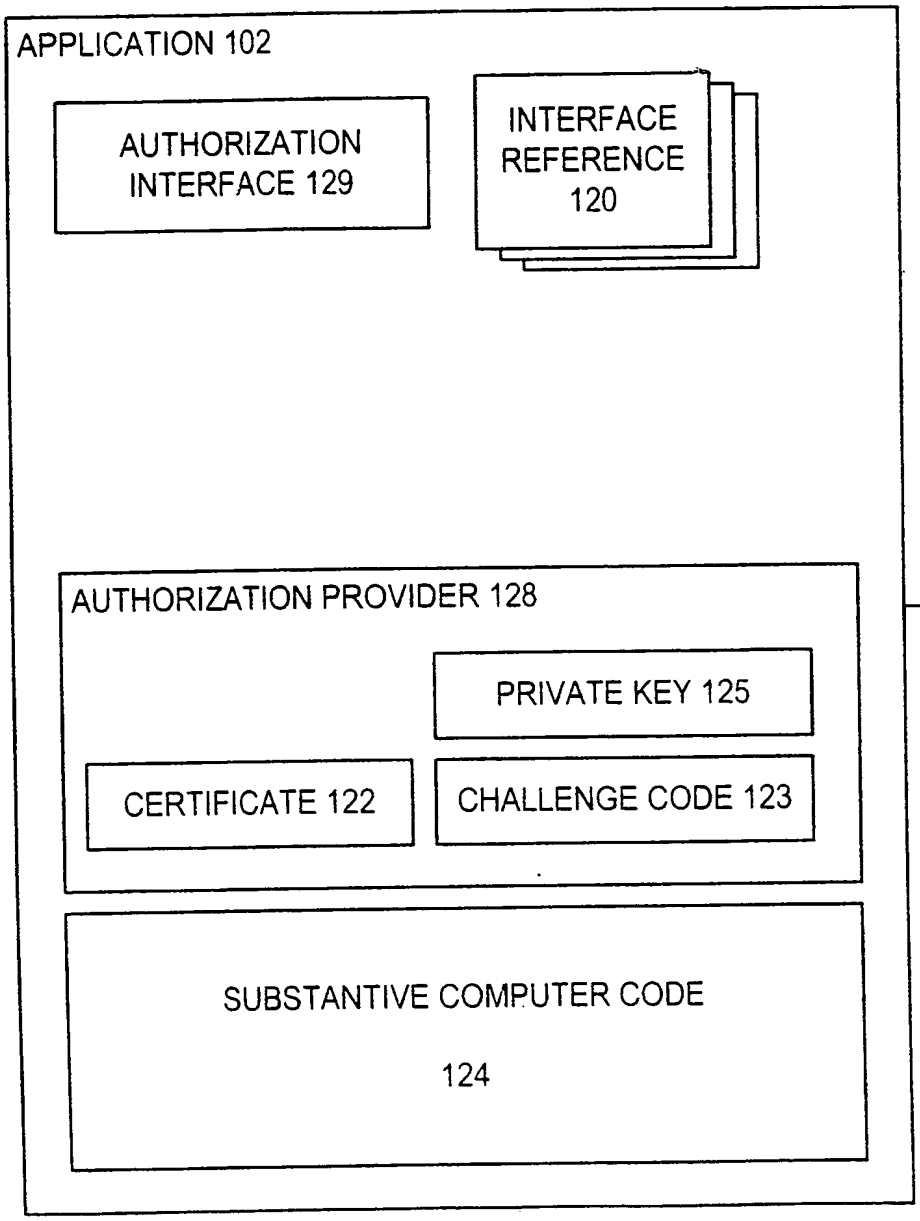
1/11

FIGURE 1A



OIPE
MAY 27 2005
PATENT & TRADEMARK OFFICE
JC37

FIGURE 1B

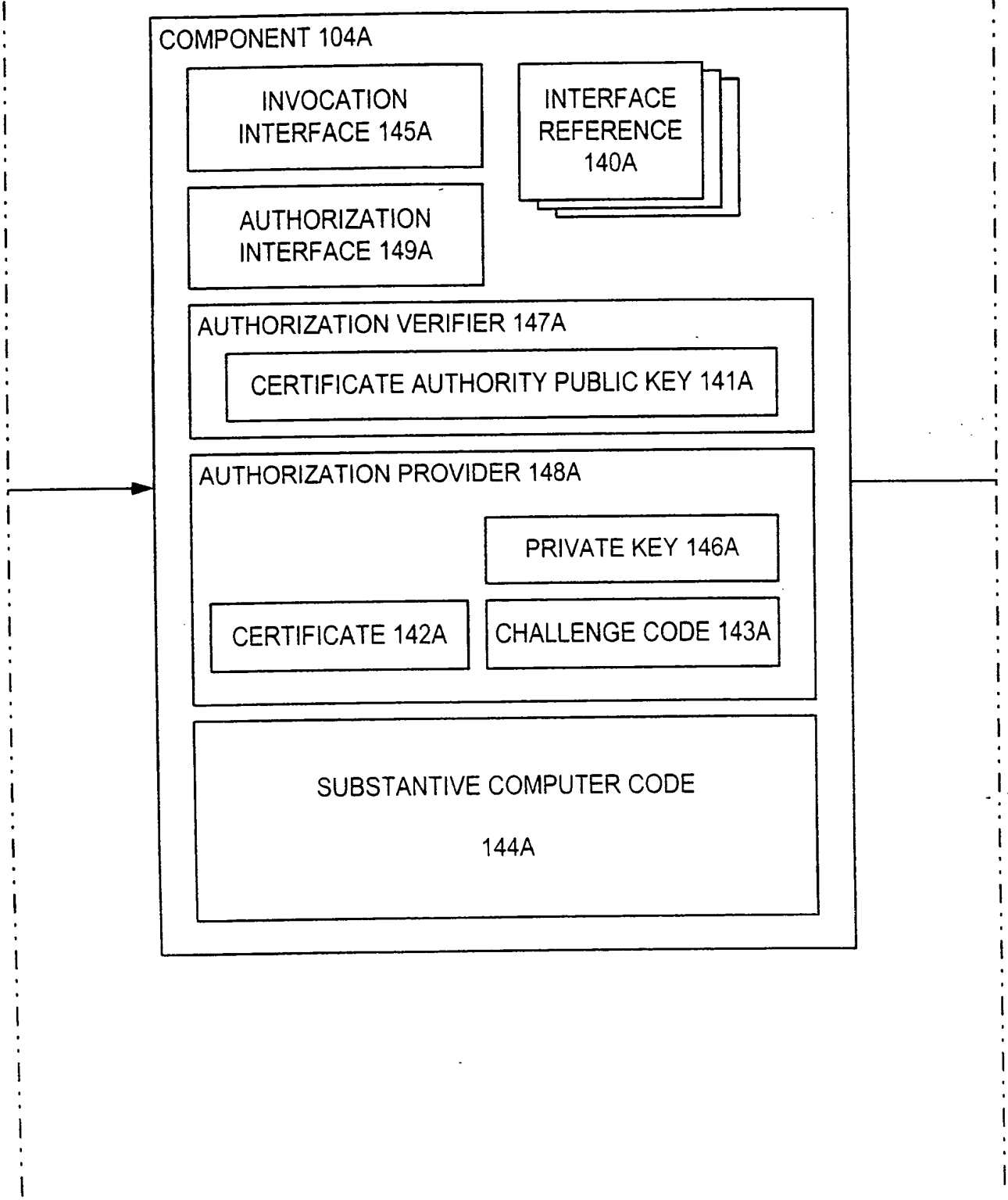

COMPONENT 104A
INVOCATION INTERFACE 145A
INTERFACE REFERENCE 140A
AUTHORIZATION INTERFACE 149A
AUTHORIZATION VERIFIER 147A
CERTIFICATE AUTHORITY PUBLIC KEY 141A
AUTHORIZATION PROVIDER 148A
PRIVATE KEY 146A
CERTIFICATE 142A
CHALLENGE CODE 143A
SUBSTANTIVE COMPUTER CODE
144A

FIGURE 1C

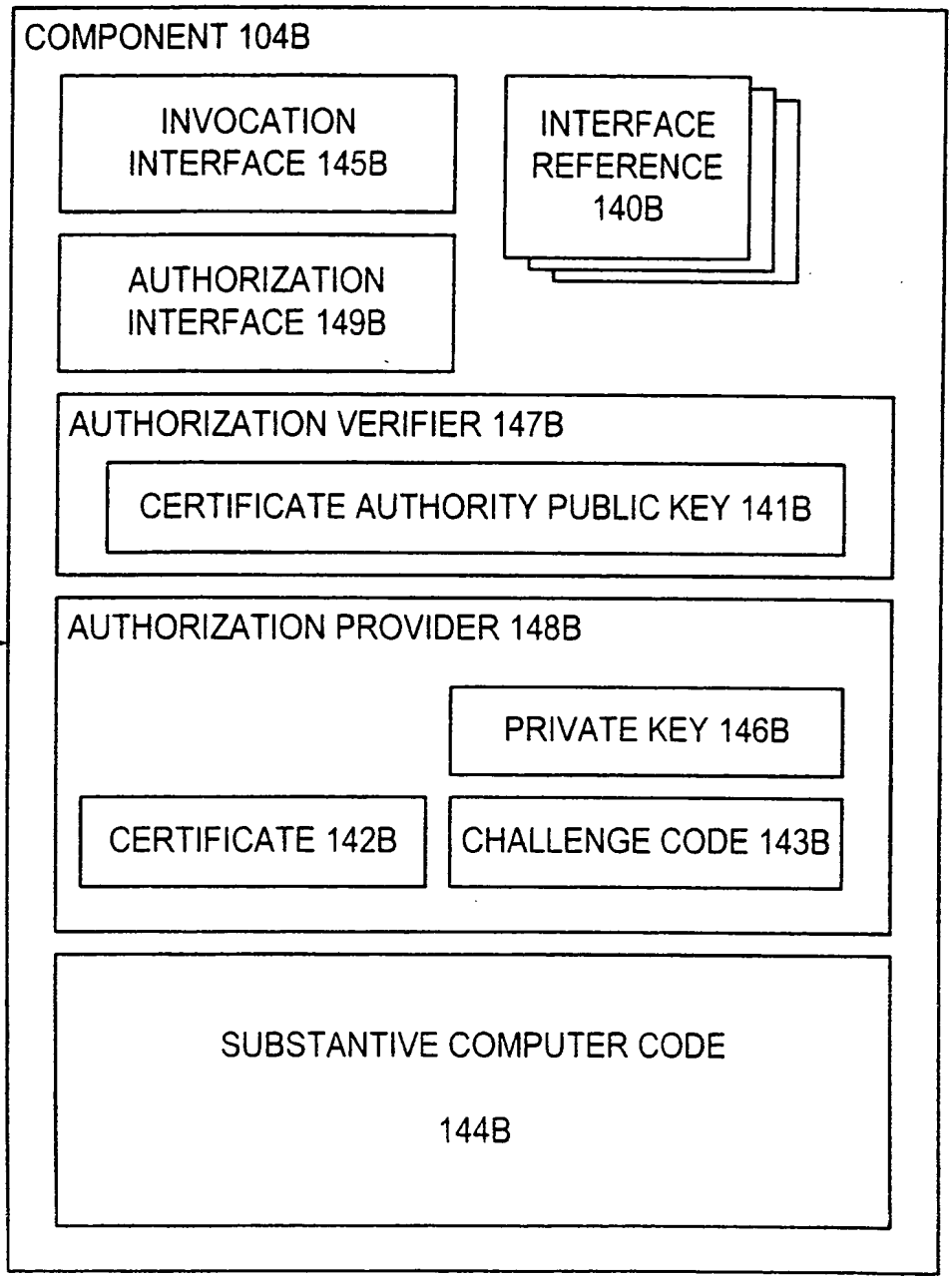


FIGURE 1A	FIGURE 1B	FIGURE 1C

FIGURE 1

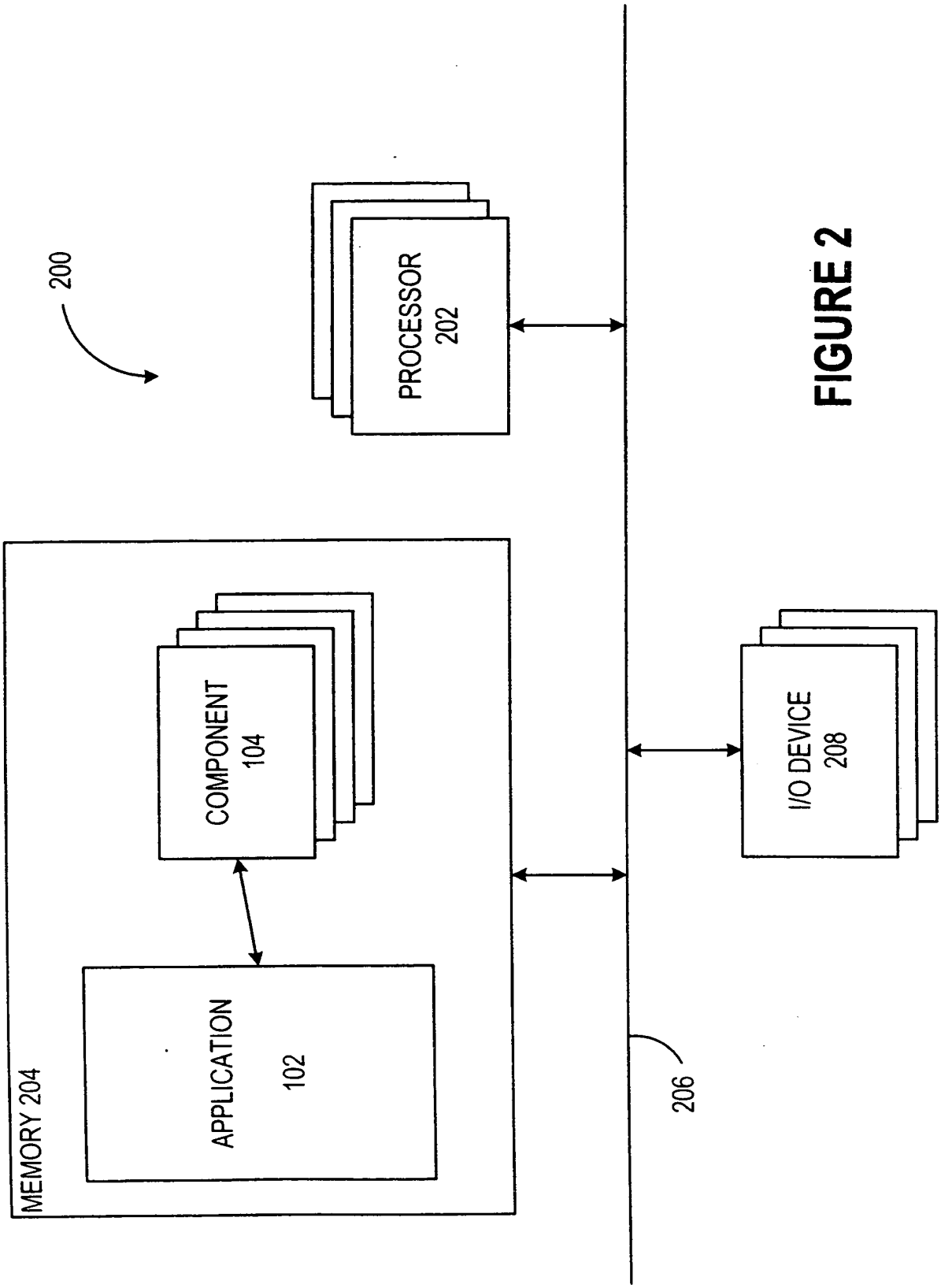

200
PROCESSOR
202
MEMORY 204
COMPONENT
104
APPLICATION
102
I/O DEVICE
208
206

FIGURE 2

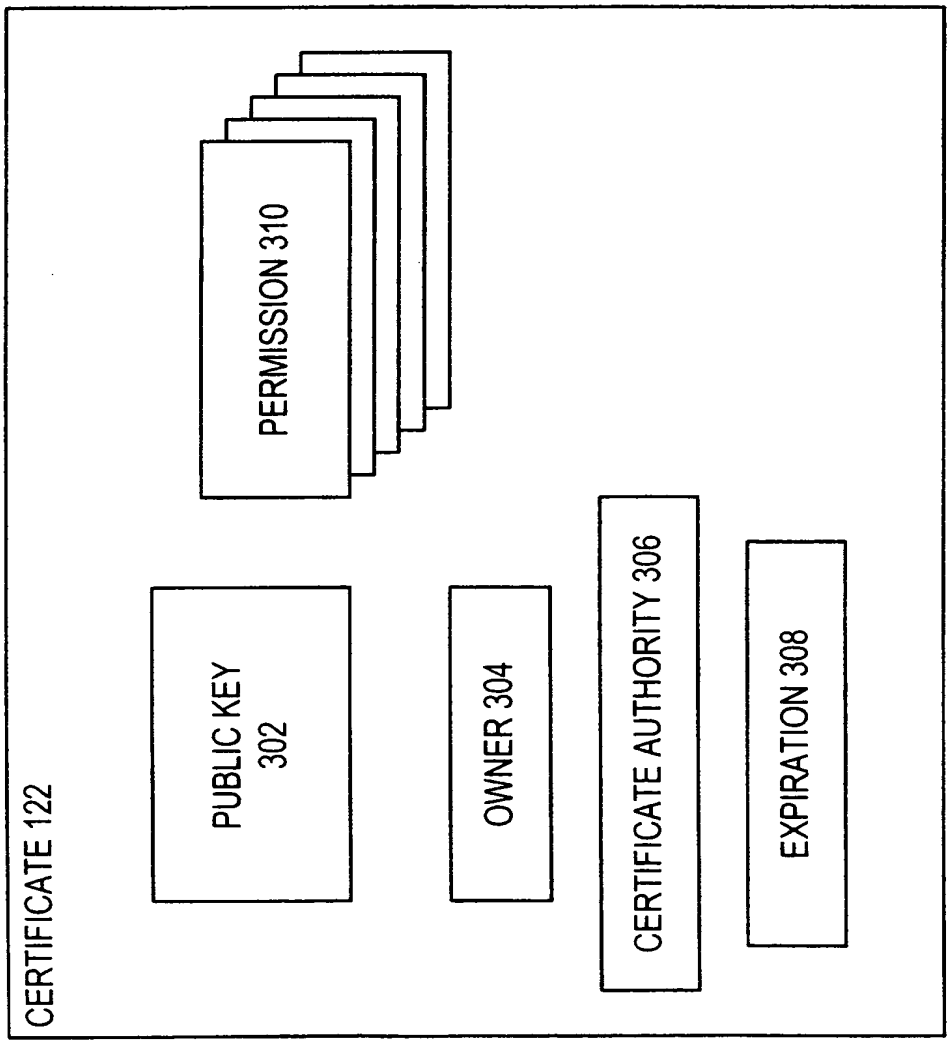

CERTIFICATE 122
PUBLIC KEY 302
PERMISSION 310
OWNER 304
CERTIFICATE AUTHORITY 306
EXPIRATION 308

FIGURE 3

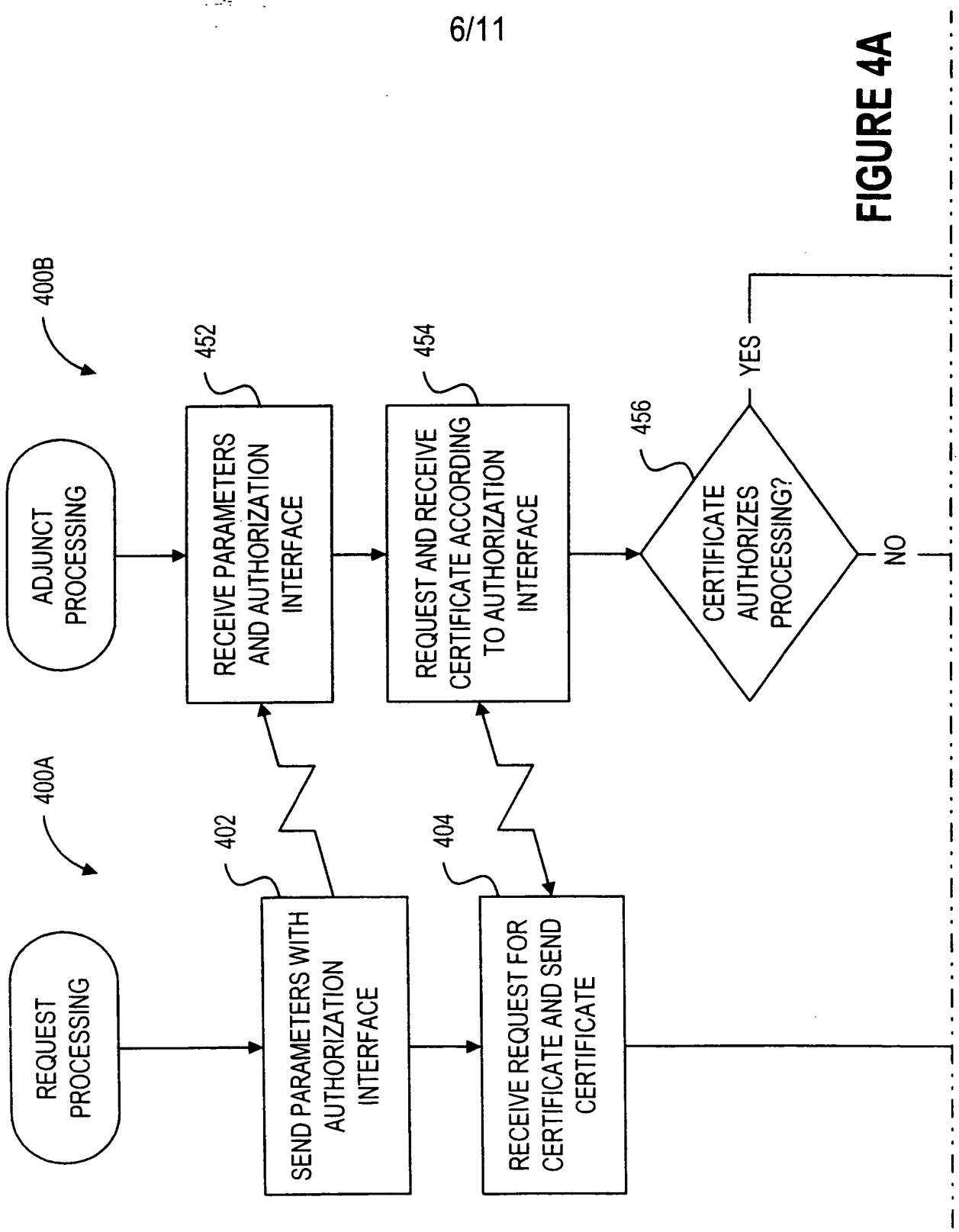

400A
REQUEST PROCESSING
402
SEND PARAMETERS WITH AUTHORIZATION INTERFACE
404
RECEIVE REQUEST FOR CERTIFICATE AND SEND CERTIFICATE
400B
ADJUNCT PROCESSING
452
RECEIVE PARAMETERS AND AUTHORIZATION INTERFACE
454
REQUEST AND RECEIVE CERTIFICATE ACCORDING TO AUTHORIZATION INTERFACE
456
CERTIFICATE AUTHORIZES PROCESSING?
YES
NO

FIGURE 4A

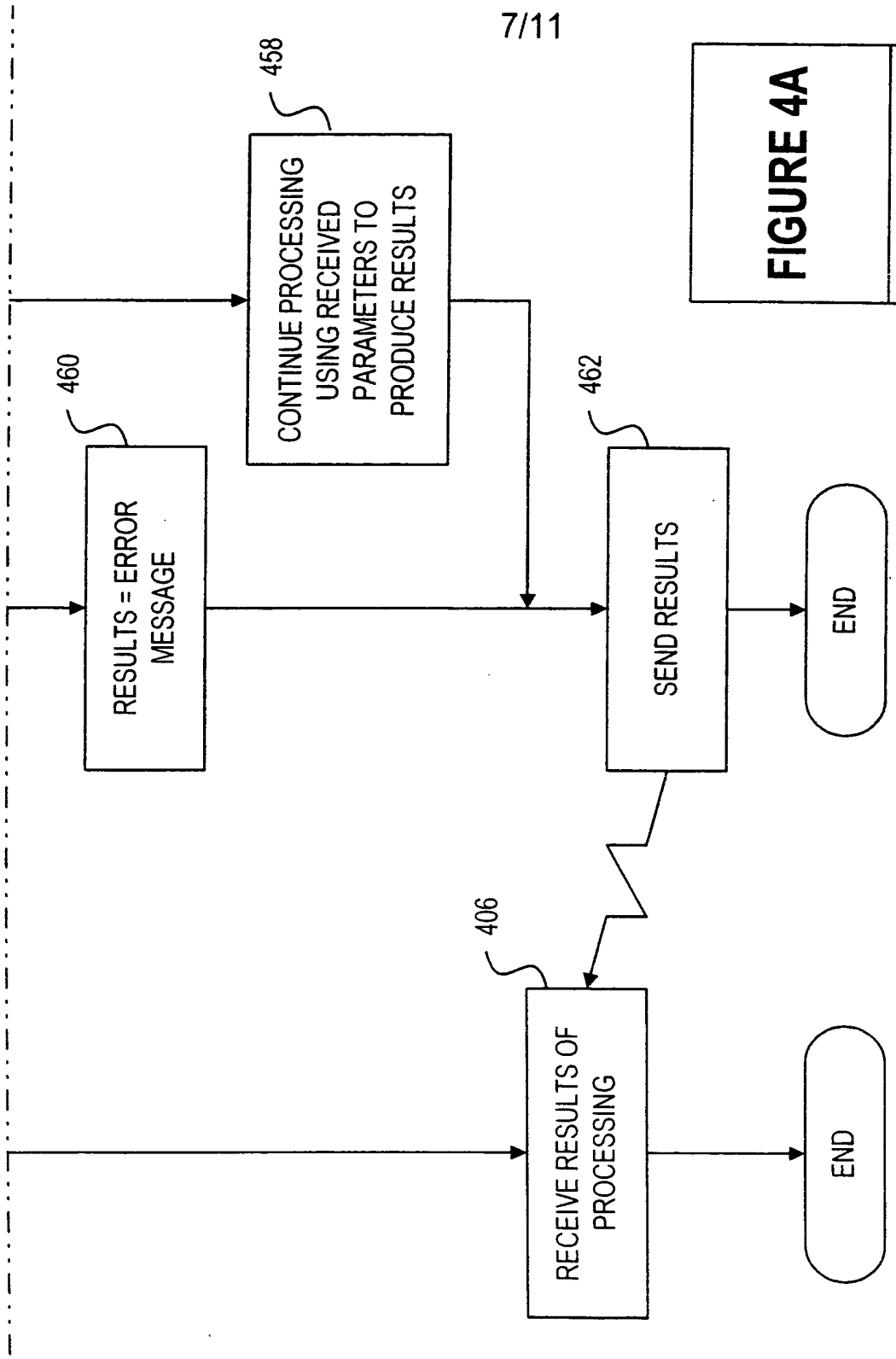


FIGURE 4A

FIGURE 4B

FIGURE 4

FIGURE 4B

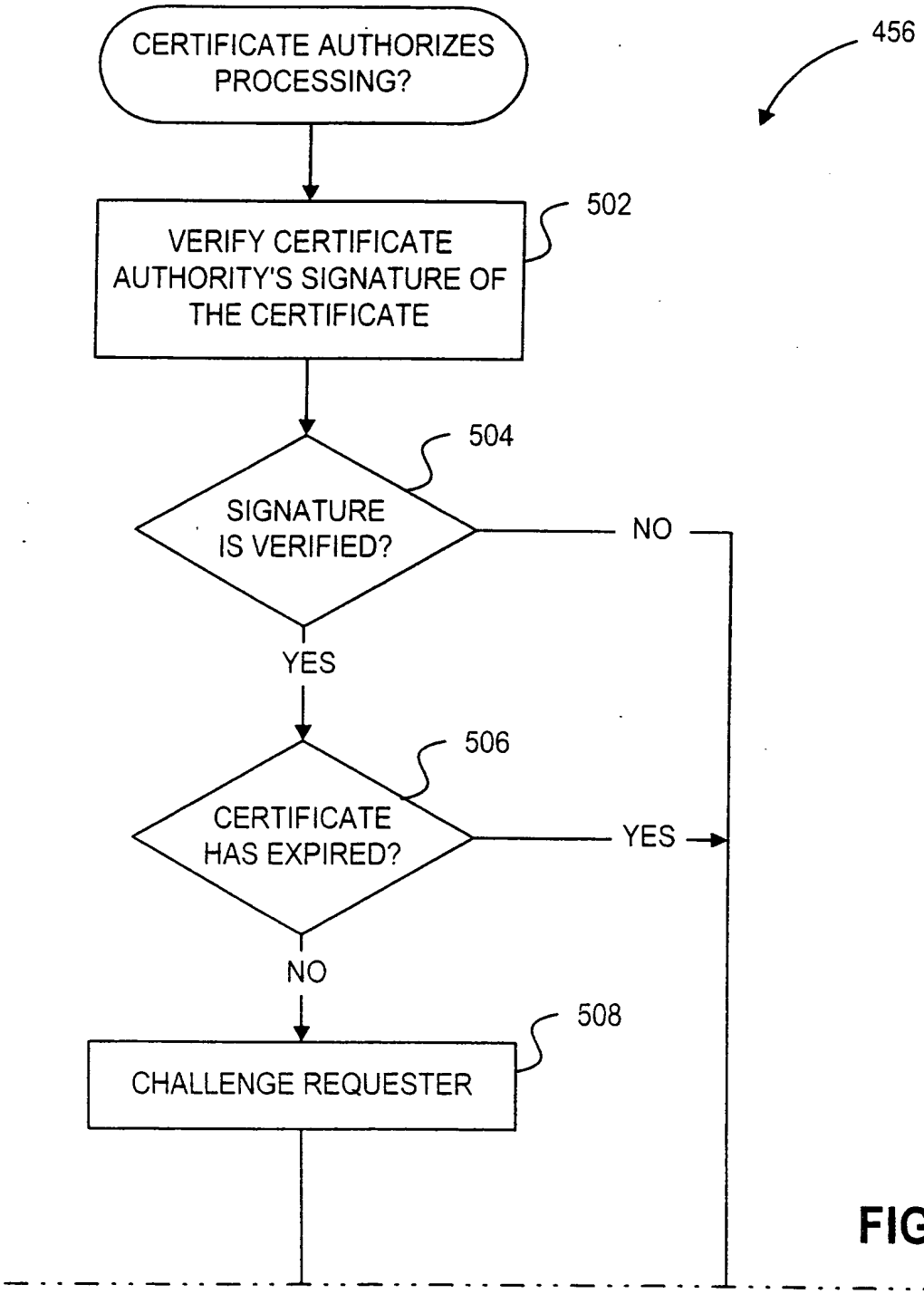

CERTIFICATE AUTHORIZES PROCESSING?
456
VERIFY CERTIFICATE AUTHORITY'S SIGNATURE OF THE CERTIFICATE
502
SIGNATURE IS VERIFIED?
504
NO
YES
CERTIFICATE HAS EXPIRED?
506
YES
NO
CHALLENGE REQUESTER
508

FIGURE 5A

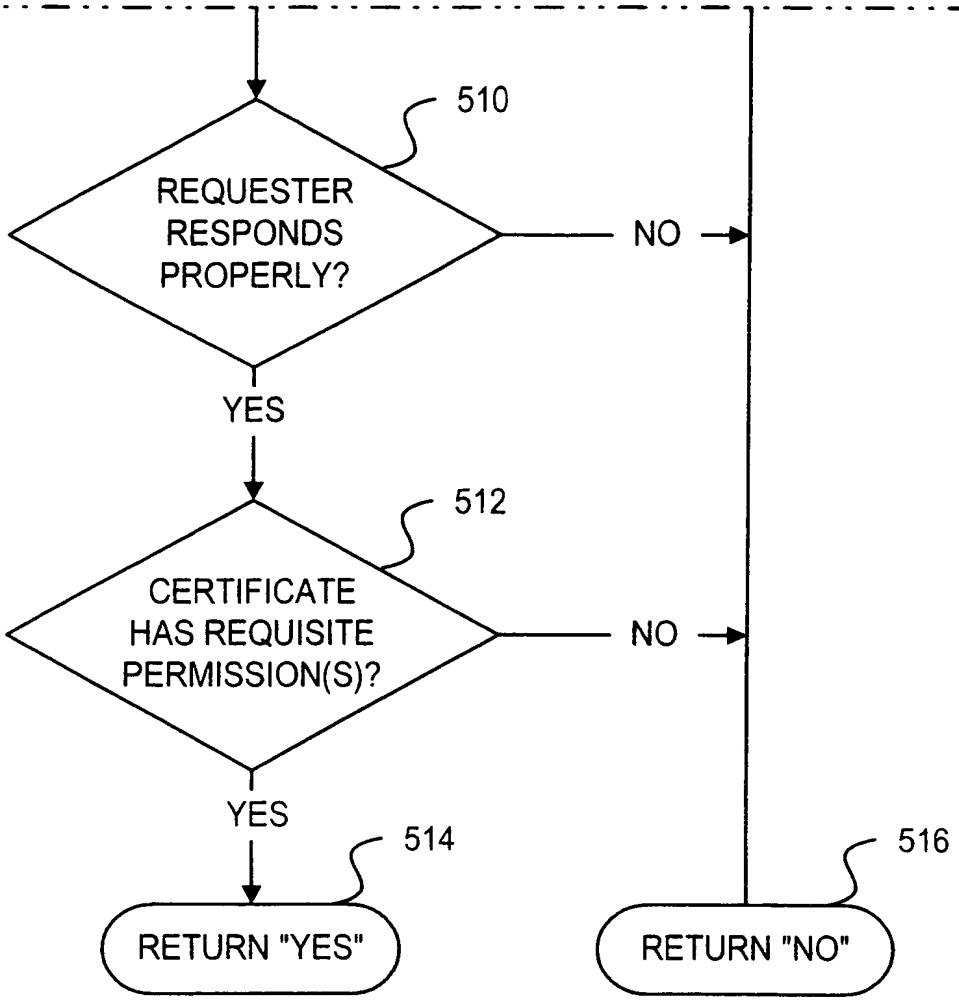


FIGURE 5B

FIGURE 5A

FIGURE 5B

FIGURE 5

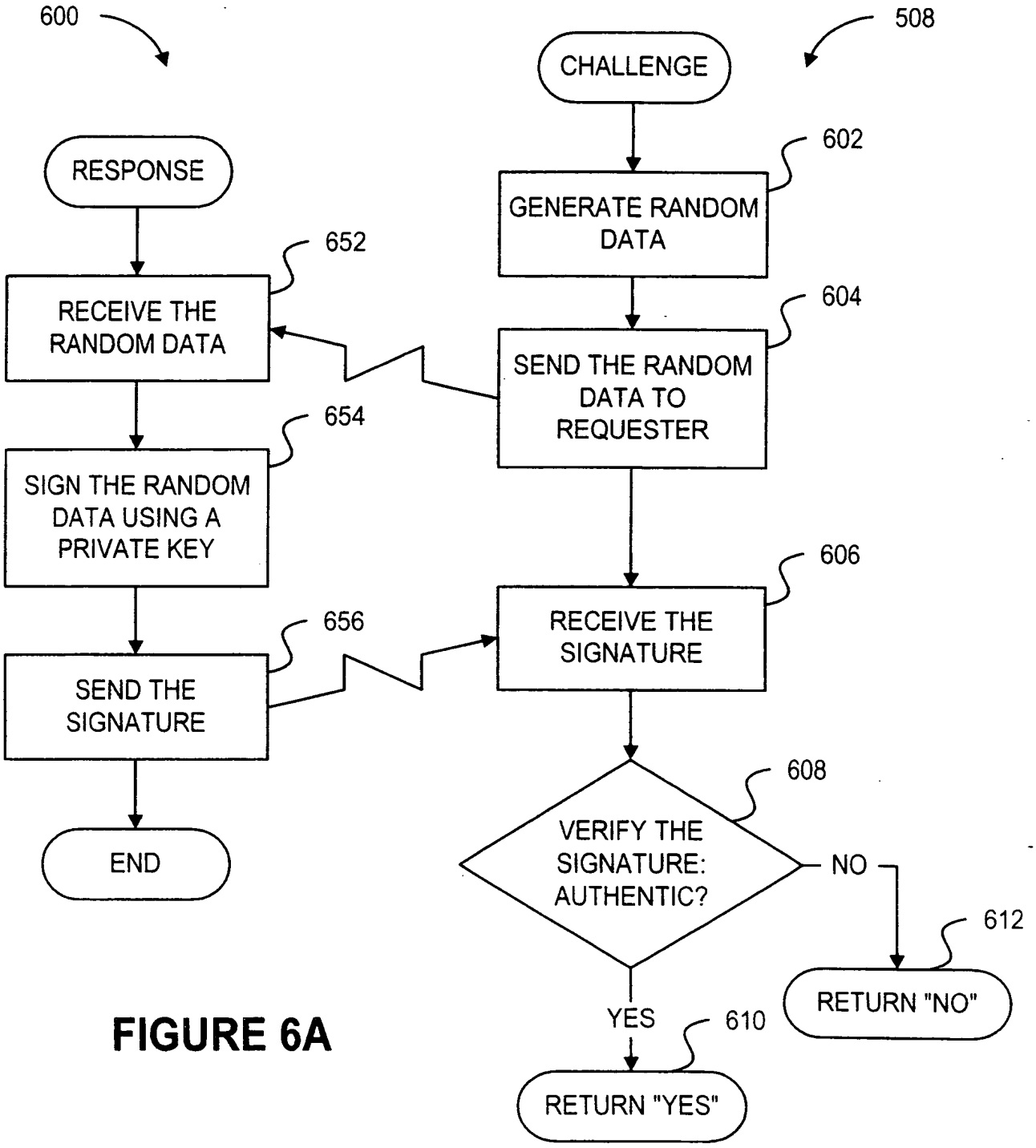

600
508
CHALLENGE
RESPONSE
602
GENERATE RANDOM DATA
652
RECEIVE THE RANDOM DATA
604
SEND THE RANDOM DATA TO REQUESTER
654
SIGN THE RANDOM DATA USING A PRIVATE KEY
606
RECEIVE THE SIGNATURE
656
SEND THE SIGNATURE
608
VERIFY THE SIGNATURE: AUTHENTIC?
NO
612
RETURN "NO"
YES
610
RETURN "YES"
END

FIGURE 6A

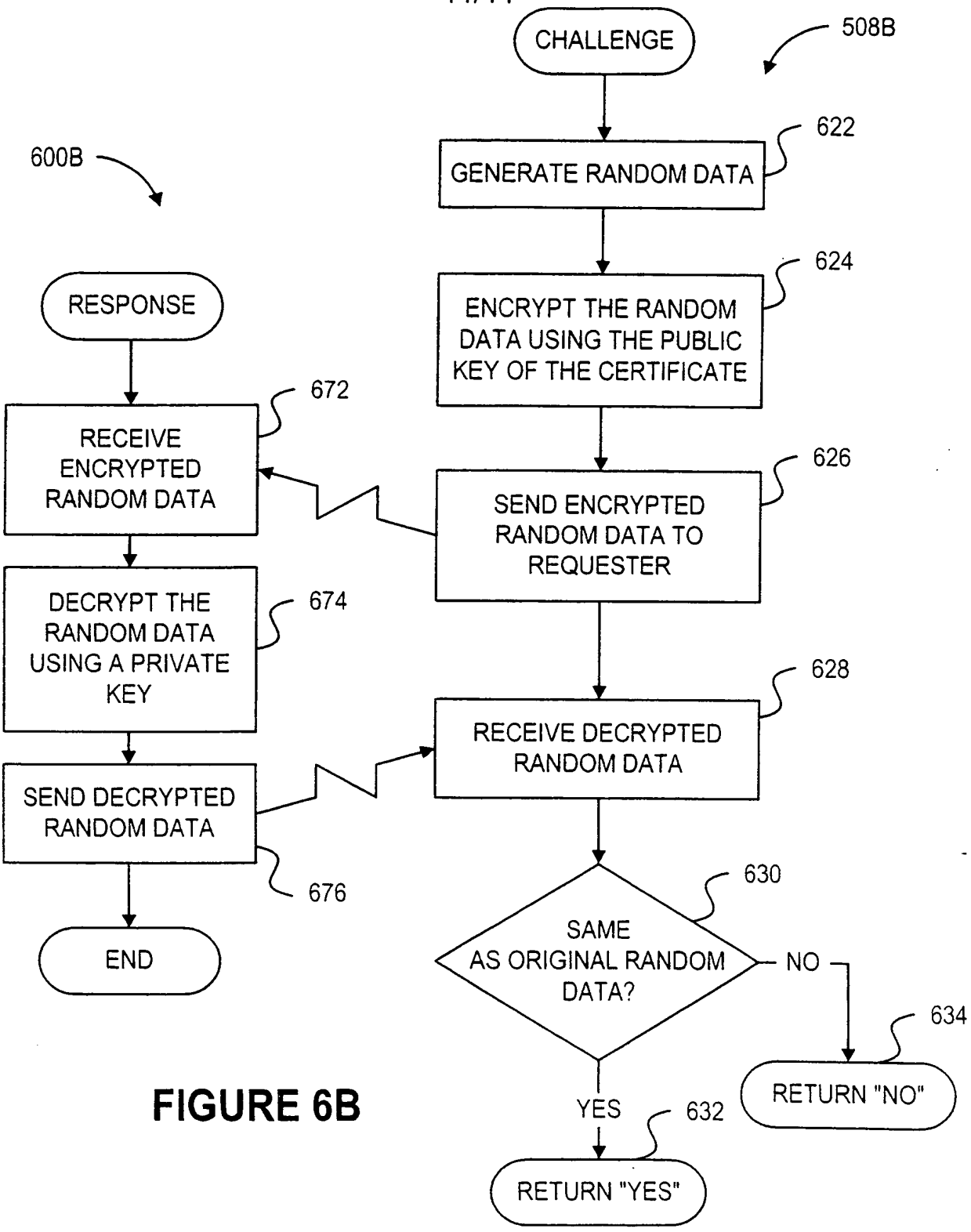

CHALLENGE
508B
600B
622
GENERATE RANDOM DATA
624
ENCRYPT THE RANDOM DATA USING THE PUBLIC KEY OF THE CERTIFICATE
RESPONSE
672
RECEIVE ENCRYPTED RANDOM DATA
626
SEND ENCRYPTED RANDOM DATA TO REQUESTER
DECRYPT THE RANDOM DATA USING A PRIVATE KEY
674
628
RECEIVE DECRYPTED RANDOM DATA
SEND DECRYPTED RANDOM DATA
676
630
SAME AS ORIGINAL RANDOM DATA?
NO
634
RETURN "NO"
END
YES
632
RETURN "YES"

FIGURE 6B